EXHIBIT 28

Unauthorized SIM Swaps

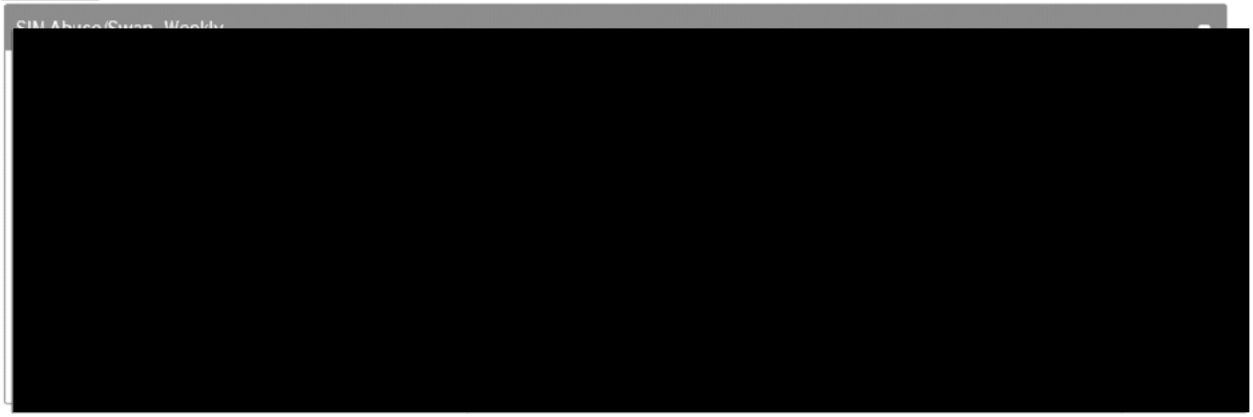
Issue:

- SMS being used as a "second step" Authentication for high profile accounts – Social Media Accounts, Crypto Currency, Financial Accounts.
- However, SMS was not designed for "proof of possession." SIM authentication is designed for this and being delivered via [redacted]

Threat Actor Tactics:

- Objective is to perform SIM Swap to enable capture of SMS bound for Victim handset.
- Method is to social engineer Authorized Retail Employees by prompting employee to visit a phishing site to harvest their credentials/Secure ID Passcode then gain OPUS access.
- Expected Tactical Migration is towards bribes/extortion and malware.

Trends:



Unauthorized SIM Swaps – decreasing due to mitigations

Detection & Mitigation Capabilities:

OPUS:

- [redacted]

CSO:

- [redacted]

[redacted]

Protection Activities Underway:

[redacted]

Tactical Recommendations:

[redacted]

ts)
s.

Strategic Recommendations:

- [redacted]
-
-

- [redacted]